Install and Setup LogAnalyzer on CentOS 8

Step 1. Install Prerequisites

In order for **LogAnalyzer** to function correctly, there are a number few required packages that need to be installed on our system.

01- Install Httpd, rsyslog-mysql packages:

```
# yum install httpd php php-cli php-common php-mysqlnd mariadb mariadb-server wget rsyslog-mysql
```

02- Make sure the **Httpd** is up and running if not run the below command:

```
# systemctl enable --now httpd
# systemctl status httpd
```

03- If the **firewalld** is installed, you have to allow the **http** protocol :

```
# firewall-cmd --permanent --add-service=http
# firewall-cmd --reload
```

Step 2. Create LogAnalyzer Database

Start and Enable MySQL Services

```
# systemctl enable --now mariadb
# systemctl status mariadb
```

01- First, import the default database scheme offered by **RSYSLOG** using the below command:

```
# mysql -u root -p < /usr/share/doc/rsyslog/mysql-createDB.sql
Enter password:
```

02- Second, let's verify if the **Syslog** database was imported correctly and create a new user:

```
# mysql -u root -p
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 20
Server version: 10.3.17-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| Syslog             |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.001 sec)

MariaDB  [(none)]>  GRANT  ALL  ON  Syslog.*  TO  'rsyslog'@'localhost'
IDENTIFIED BY 'Password';
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> exit
Bye
```

Step 3. Configure Rsyslog Server

01- To start, we need to configure **Rsyslog** server to accept **syslog** from remote servers. First, make sure to backup your rsyslog configuration File:

```
# cp /etc/rsyslog.conf /etc/rsyslog.conf.ori
```

02- Now, find and uncomment the following lines to make your the **Rsyslog** server to listen on the **udp** and **tcp** ports.

```
# vi /etc/rsyslog.conf

[...]
# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")
```

03- To forward logs into **MySQL/MariaDB** database. So, add the following lines to enable **ommysql module** and to create a new forwarding rule:

```
# Load the MySQL Module
module(load="ommysql")

#*.* :ommysql:127.0.0.1,Syslog_Database,syslog_user,password
*.* :ommysql:127.0.0.1,Syslog,rsyslog,Password
```

Rsyslog is now ready to receive logs and forward them to MySQL database. However, you might need to restrict log forwarding to Rsyslog using the **$AllowedSender** parameter.

This parameter takes the format;

```
$AllowedSender [UDP/TCP], ip[/bits], ip[/bits]
```

Hence, to allow specific servers to send logs to Rsyslog server, you would simply add a line like as shown below under the **### GLOBAL DIRECTIVES ###** section.

```
$AllowedSender UDP, 192.168.20.0/24
```

To define servers allowed for TCP syslog reception;

```
$AllowedSender TCP, 192.168.20.0/24
```

04- After, you finished editing the file. Save and restart the **rsyslog** service

```
# systemctl restart rsyslog
```

05- If the **firewalld** is installed, you have to allow the following ports to enable to receive logs from remote servers:

```
# firewall-cmd --add-port=514/{tcp,udp} --permanent
# firewall-cmd --reload
```

Step 4. Install LogAnalyzer

01- First go to the official Adiscon Loganlayzer website and download the most recent version of the software to your server.

```
# wget http://download.adiscon.com/loganalyzer/loganalyzer-4.1.12.tar.gz -P /tmp
# tar -xzvf /tmp/loganalyzer-4.1.12.tar.gz -C /opt/
```

02- Create the **LogAnalyzer** directory under the apache web directory:

```
[root@loganalyzer ~]# mkdir /var/www/html/loganalyzer
```

03- Copy the installation files into **loganalyzer** directory using the following commands:

```
# cp -r /opt/loganalyzer-4.1.12/src/* /var/www/html/loganalyzer
# cp /opt/loganalyzer-4.1.12/contrib/configure.sh /var/www/html/loganalyzer
```

04- Create a blank configuration file named config.php in **loganalyzer** directory the following commands:

```
# cd /var/www/html/loganalyzer
# bash configure.sh
```

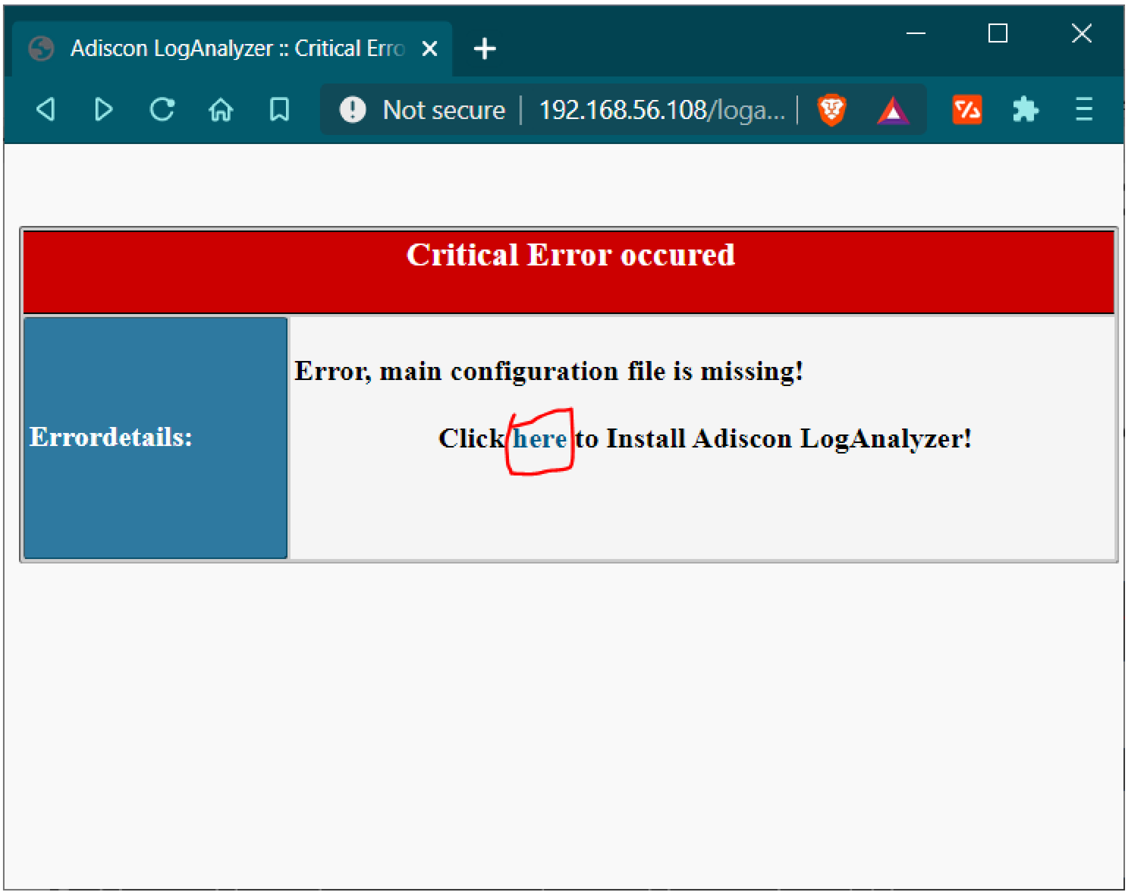
Step 5: Configure web server

```
# vi /etc/httpd/conf.d/loganalyzer.conf

 Alias /loganalyzer /var/www/html/loganalyzer

#systemctl restart httpd
```

Step 5. start LogAnalyzer web installer

01- After completing above steps open following url in your favorite web browser to start **LogAnalyzer** web installer.

```
http://localhost/loganalyzer
```



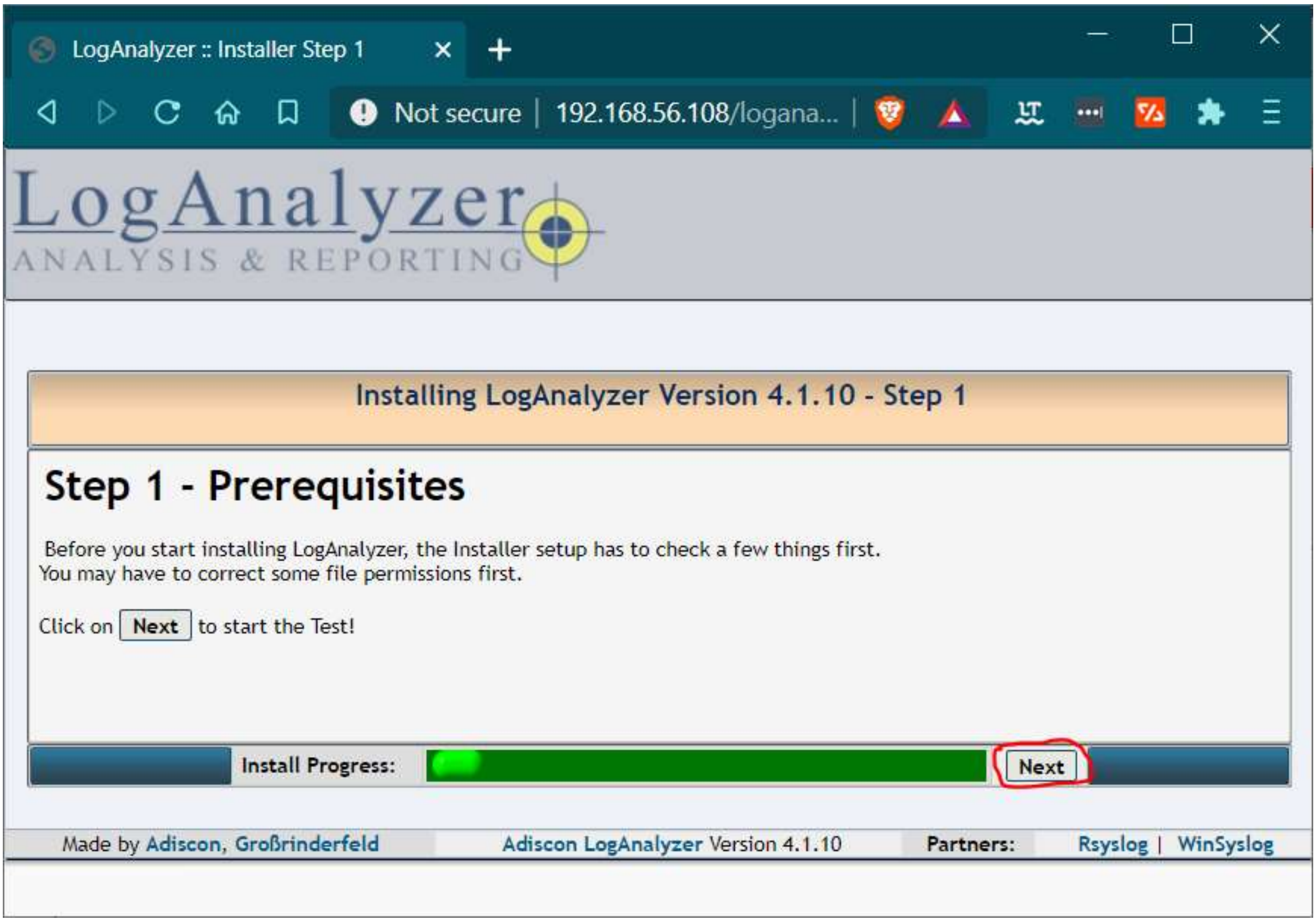
Adiscon LogAnalyzer :: Critical Erro
Not secure | 192.168.56.108/loga...

Critical Error occured

Errordetails:

Error, main configuration file is missing!

Click here to Install Adiscon LogAnalyzer!



LogAnalyzer :: Installer Step 1
Not secure | 192.168.56.108/logana...
LogAnalyzer
ANALYSIS & REPORTING

Installing LogAnalyzer Version 4.1.10 - Step 1

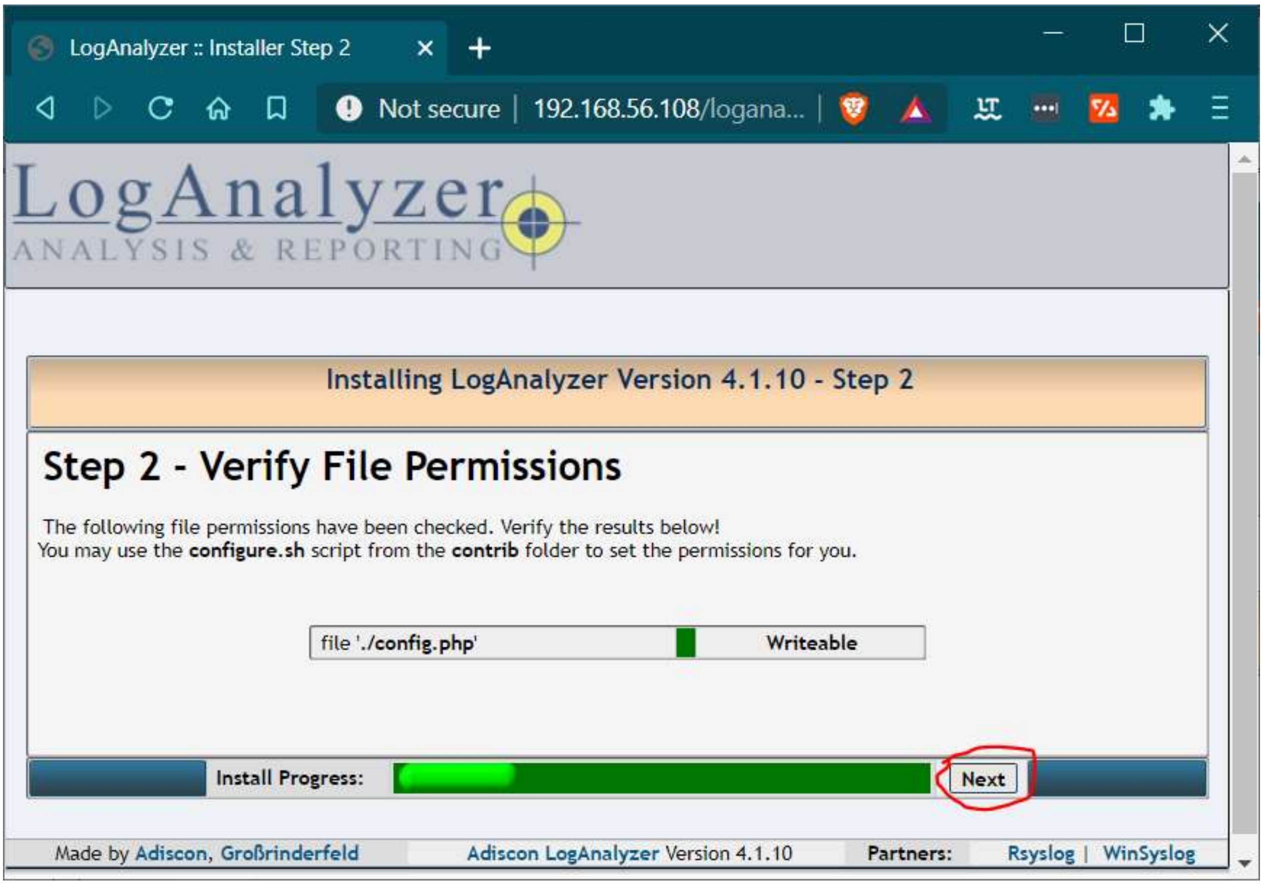
Step 1 - Prerequisites

Before you start installing LogAnalyzer, the Installer setup has to check a few things first.
You may have to correct some file permissions first.

Click on Next to start the Test!

Install Progress: Next

Made by Adiscon, Großrinderfeld   Adiscon LogAnalyzer Version 4.1.10   Partners: Rsyslog | WinSyslog


LogAnalyzer :: Installer Step 2
Not secure | 192.168.56.108/logana...
LogAnalyzer
ANALYSIS & REPORTING

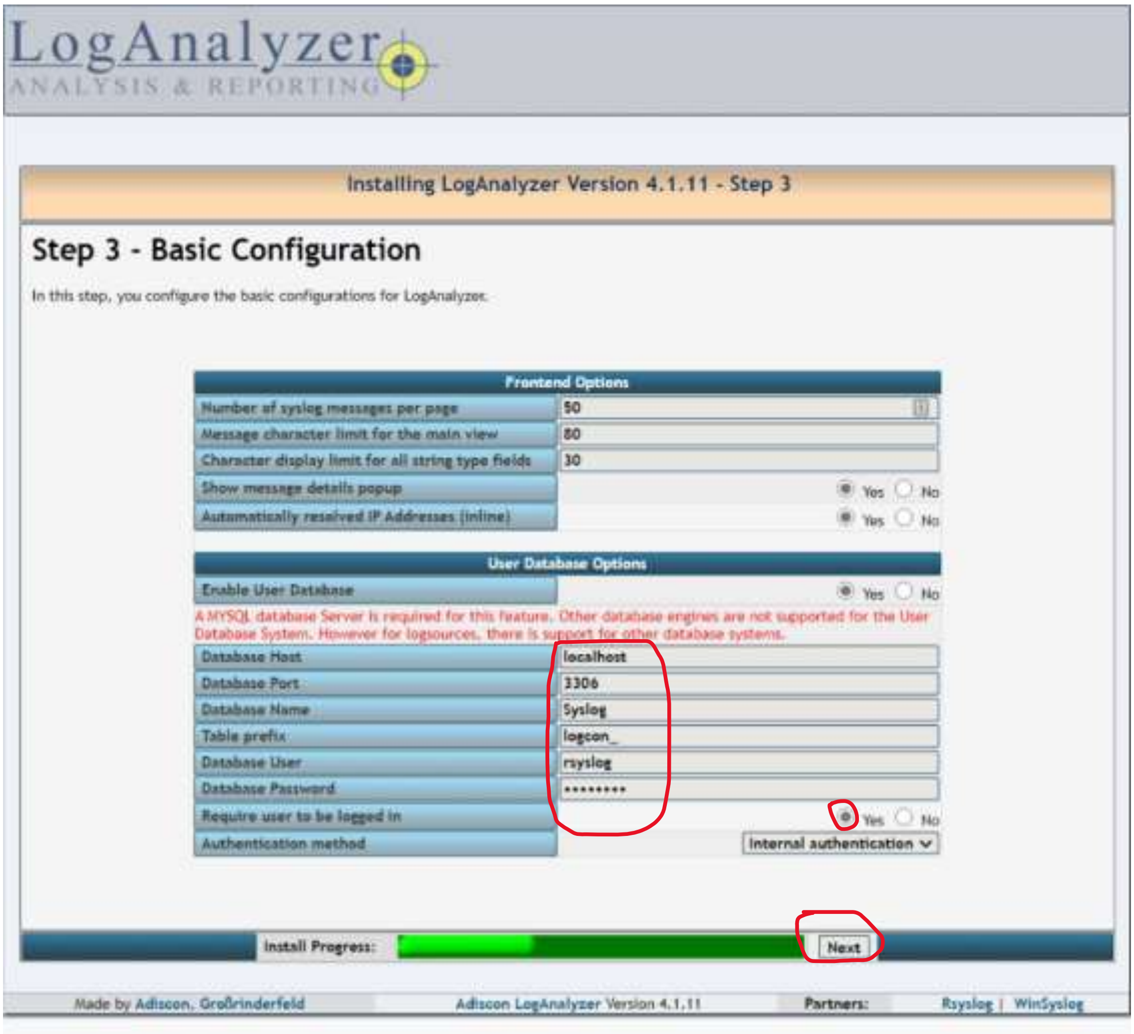
Installing LogAnalyzer Version 4.1.10 - Step 2

Step 2 - Verify File Permissions

The following file permissions have been checked. Verify the results below!
You may use the **configure.sh** script from the **contrib** folder to set the permissions for you.

file './config.php'	🟩 Writeable

Install Progress:
Next
Made by Adiscon, Großrinderfeld
Adiscon LogAnalyzer Version 4.1.10
Partners:
Rsyslog | WinSyslog



Installing LogAnalyzer Version 4.1.11 - Step 3

Step 3 - Basic Configuration

In this step, you configure the basic configurations for LogAnalyzer.

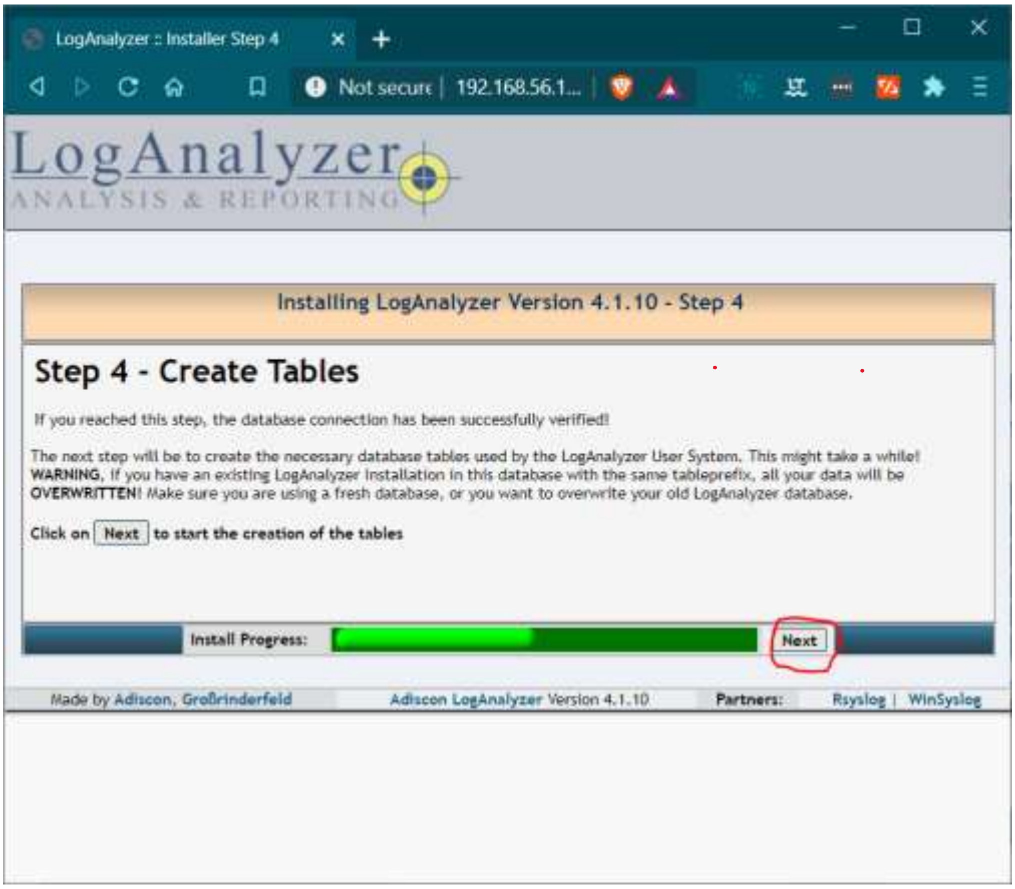
Frontend Options	
Number of syslog messages per page	50
Message character limit for the main view	80
Character display limit for all string type fields	30
Show message details popup	● Yes ○ No
Automatically resolved IP Addresses (inline)	● Yes ○ No

User Database Options	
Enable User Database	● Yes ○ No

A MYSQL database Server is required for this feature. Other database engines are not supported for the User Database System. However for logsources, there is support for other database systems.

Database Host	localhost
Database Port	3306
Database Name	Syslog
Table prefix	logcon_
Database User	rsyslog
Database Password	********
Require user to be logged in	● Yes ○ No
Authentication method	Internal authentication

Install Progress:
Next
Made by Adiscon, Großrinderfeld
Adiscon LogAnalyzer Version 4.1.11
Partners:
Rsyslog | WinSyslog



Installing LogAnalyzer Version 4.1.10 - Step 4

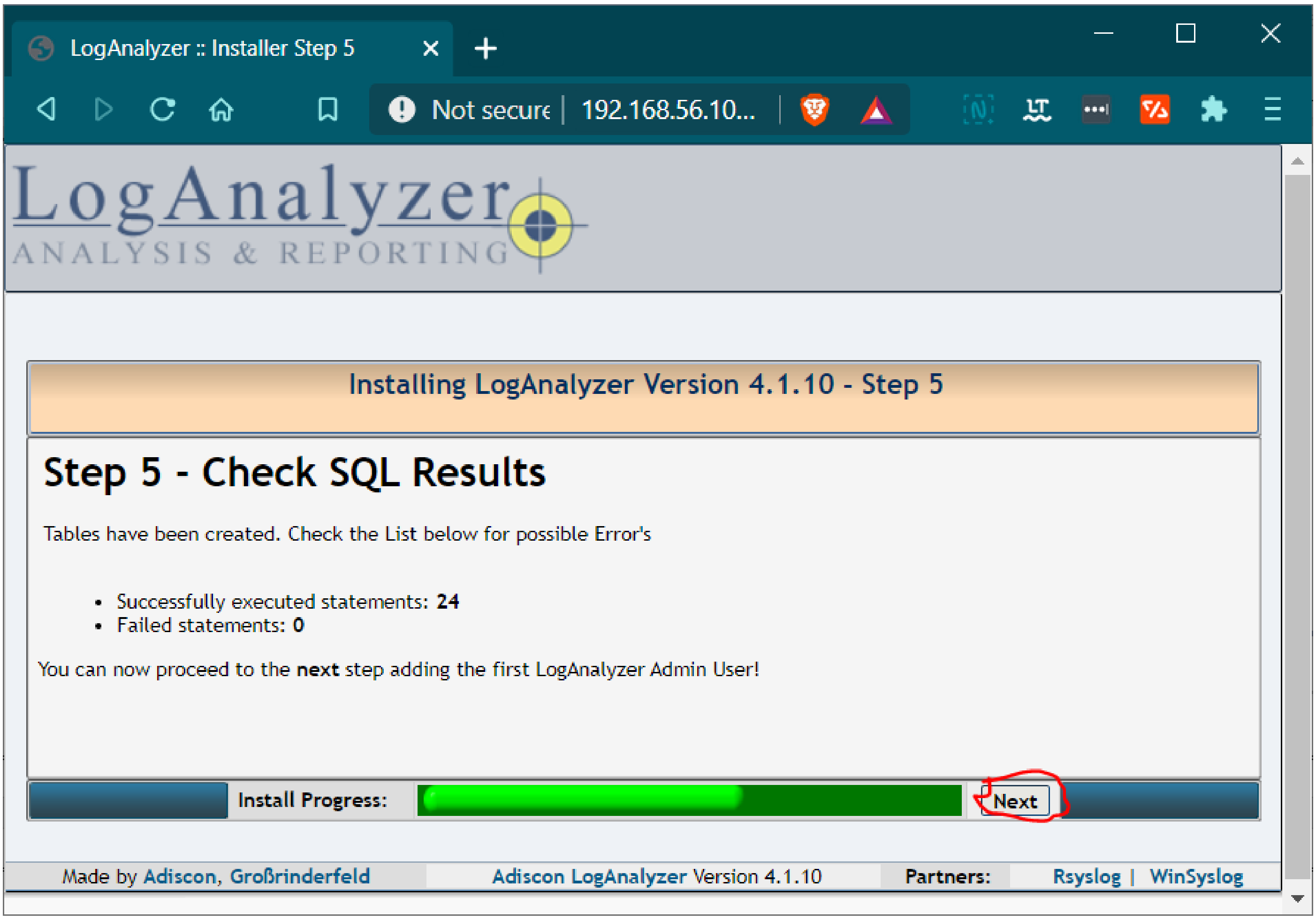
Step 4 - Create Tables

If you reached this step, the database connection has been successfully verified!

The next step will be to create the necessary database tables used by the LogAnalyzer User System. This might take a while! **WARNING**, if you have an existing LogAnalyzer installation in this database with the same tableprefix, all your data will be **OVERWRITTEN**! Make sure you are using a fresh database, or you want to overwrite your old LogAnalyzer database.

Click on Next to start the creation of the tables

Install Progress:
Next
Made by Adiscon, Großrinderfeld
Adiscon LogAnalyzer Version 4.1.10
Partners:
Rsyslog | WinSyslog


LogAnalyzer :: Installer Step 5
Not secure | 192.168.56.10...
LogAnalyzer
ANALYSIS & REPORTING

Installing LogAnalyzer Version 4.1.10 - Step 5

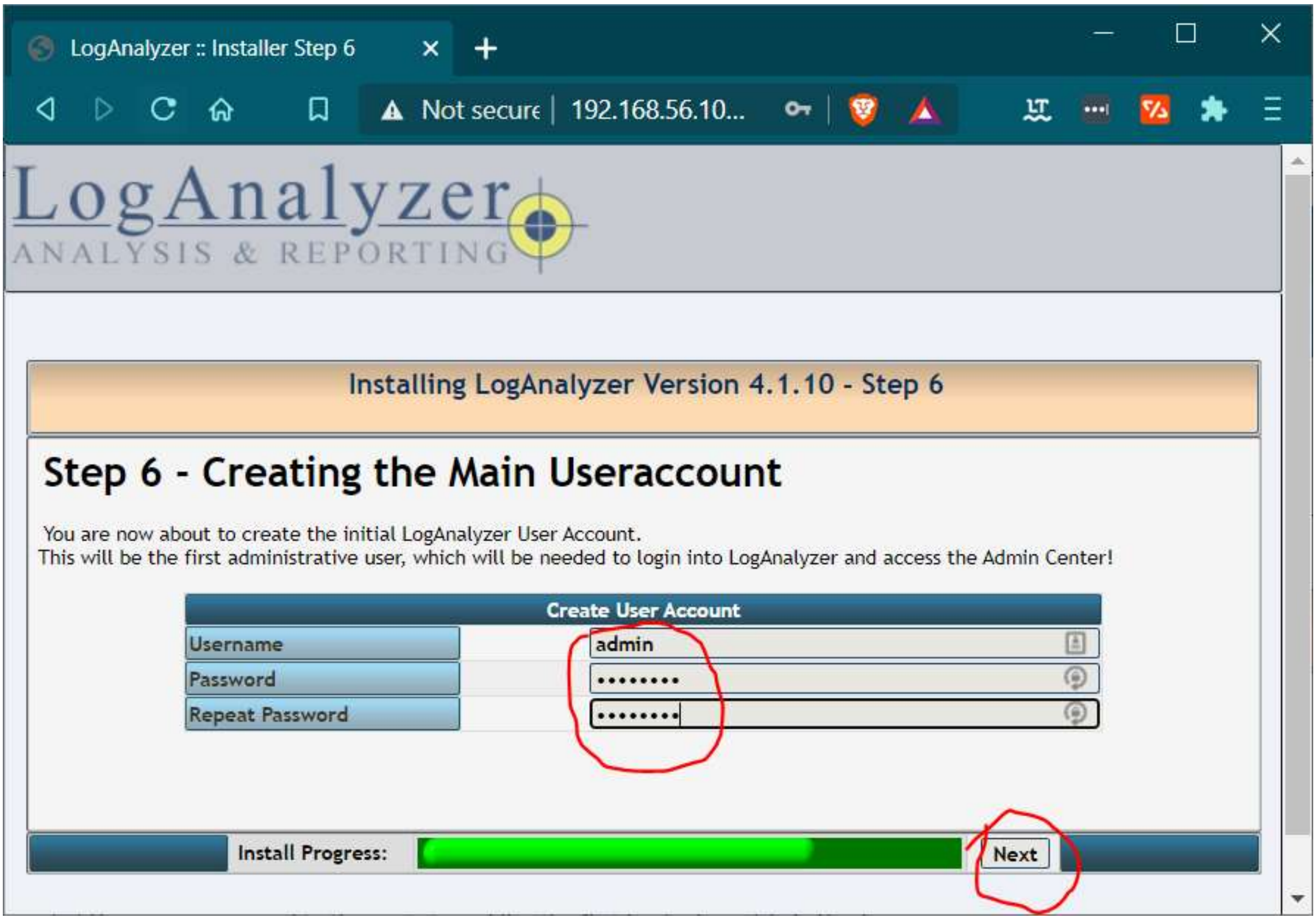
Step 5 - Check SQL Results

Tables have been created. Check the List below for possible Error's

- Successfully executed statements: **24**
- Failed statements: **0**

You can now proceed to the **next** step adding the first LogAnalyzer Admin User!

Install Progress:
Next
Made by Adiscon, Großrinderfeld
Adiscon LogAnalyzer Version 4.1.10
Partners:
Rsyslog | WinSyslog



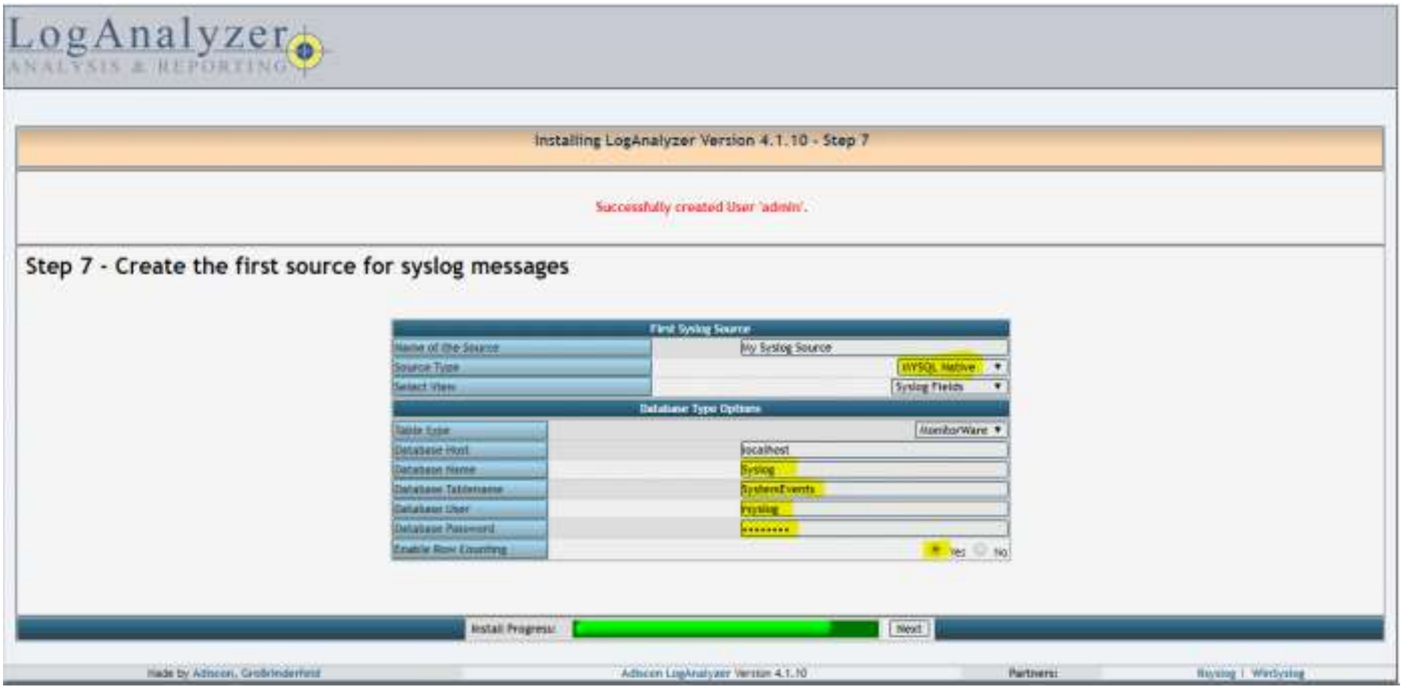
Installing LogAnalyzer Version 4.1.10 - Step 6

Step 6 - Creating the Main Useraccount

You are now about to create the initial LogAnalyzer User Account.
This will be the first administrative user, which will be needed to login into LogAnalyzer and access the Admin Center!

Create User Account	
Username	admin
Password	••••••••
Repeat Password	••••••••

Install Progress:



Installing LogAnalyzer Version 4.1.10 - Step 7

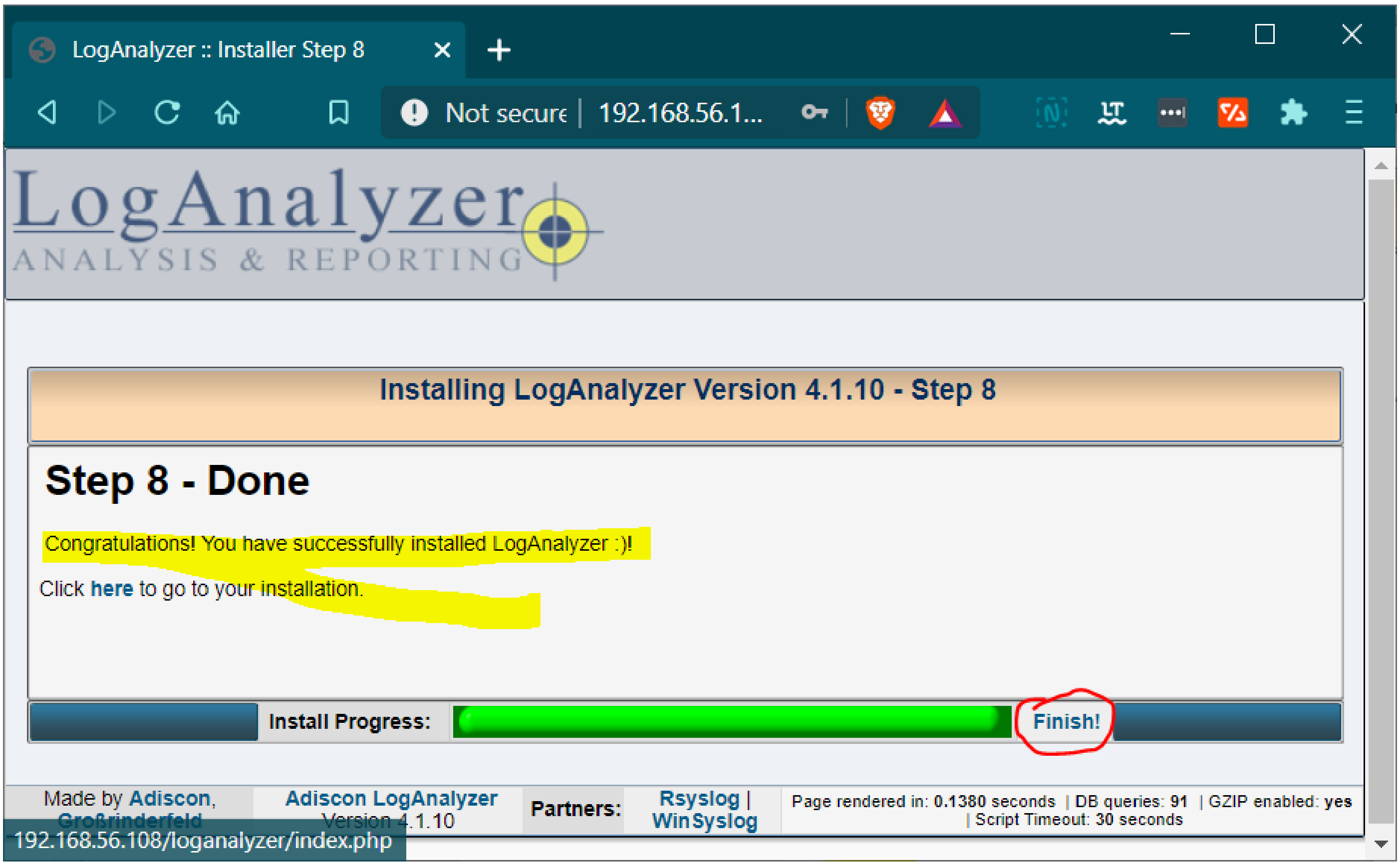
Successfully created User 'admin'.

Step 7 - Create the first source for syslog messages

First Syslog Source	
Name of the Source	My Syslog Source
Source Type	MYSQL Native
Select View	Syslog Fields
Database Type Options	
Table type	MonitorWare
Database Host	localhost
Database Name	Syslog
Database Tablename	SystemEvents
Database User	rsyslog
Database Password	••••••••
Enable Row Counting	● Yes ○ No

Install Progress:

Next
Made by Adiscon, Großrinderfeld
Adiscon LogAnalyzer Version 4.1.10
Partners:
Rsyslog | WinSyslog


LogAnalyzer :: Installer Step 8
Not secure | 192.168.56.1...
LogAnalyzer
ANALYSIS & REPORTING

Installing LogAnalyzer Version 4.1.10 - Step 8

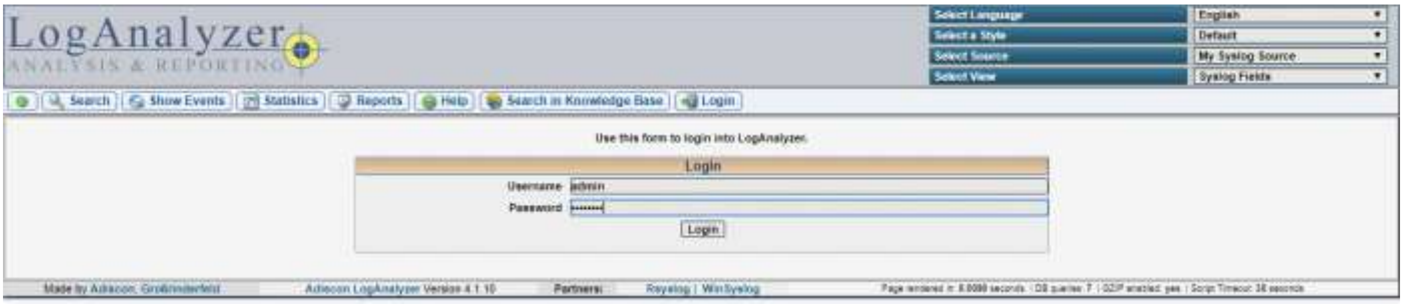
Step 8 - Done

Congratulations! You have successfully installed LogAnalyzer :)!

Click here to go to your installation.

Install Progress: Finish!

Made by Adiscon, Großrinderfeld
Adiscon LogAnalyzer Version 4.1.10
Partners: Rsyslog | WinSyslog
Page rendered in: 0.1380 seconds | DB queries: 91 | GZIP enabled: yes | Script Timeout: 30 seconds
192.168.56.108/loganalyzer/index.php


LogAnalyzer
ANALYSIS & REPORTING
Select Language
Select a Style
Select Source
Select View
Search
Show Events
Statistics
Reports
Help
Search in Knowledge Base
Login

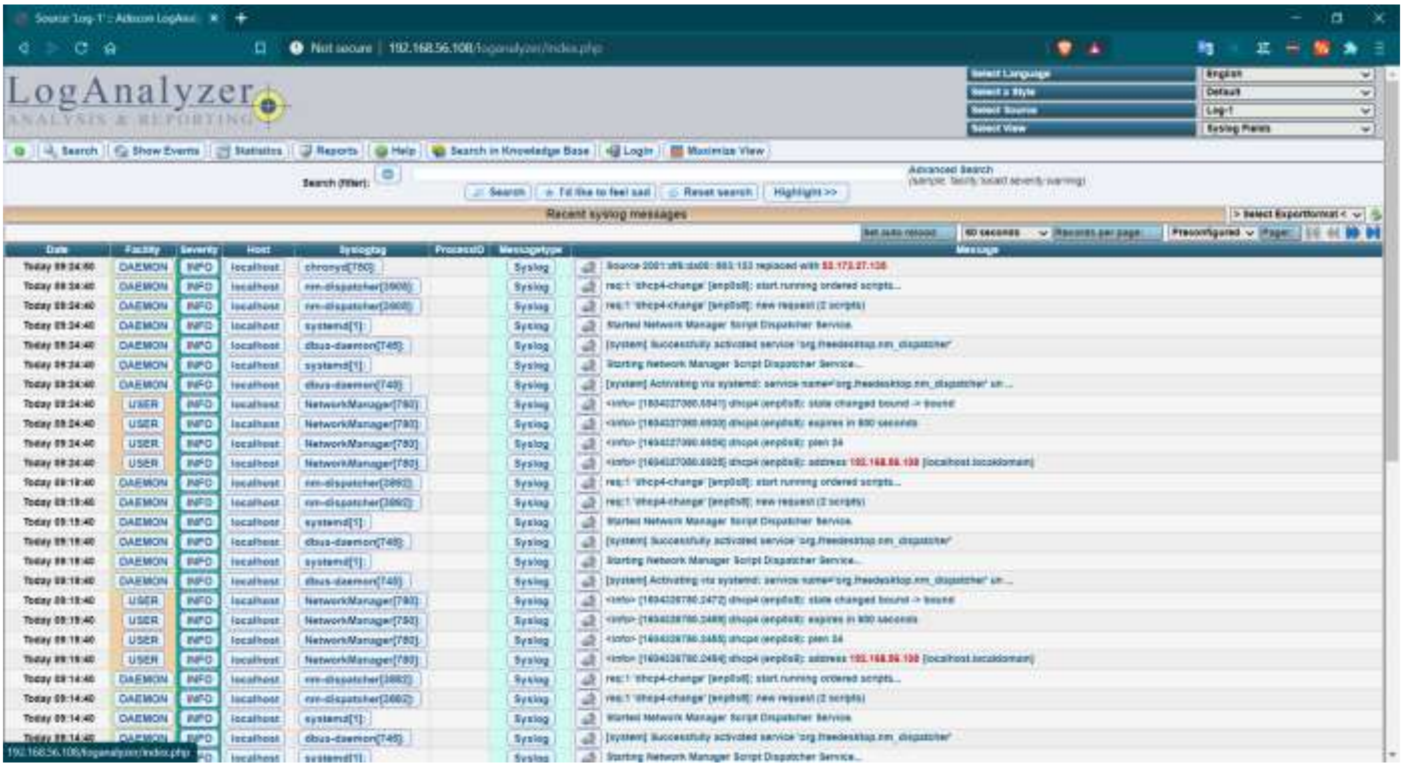
Select Language: English
Select a Style: Default
Select Source: My Syslog Source
Select View: Syslog Fields

Use this form to login into LogAnalyzer.

Login

Username: admin
Password: ••••••••

Login
Made by Adiscon, Großrinderfeld
Adiscon LogAnalyzer Version 4.1.10
Partners: Rsyslog | WinSyslog
Page rendered in: 0.0099 seconds | DB queries: 7 | GZIP enabled: yes | Script Timeout: 30 seconds



Select Language: English
Select a Style: Default
Select Source: Log-1
Select View: Syslog Fields

Search (filter):

60 seconds | Preconfigured

Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 09:24:40	DAEMON	INFO	localhost	chronyd[780]:		Syslog	Source 2001:df8:da00::883:153 replaced with 52.173.27.138
Today 09:24:40	DAEMON	INFO	localhost	nm-dispatcher[3900]:		Syslog	req:1 'dhcp4-change' [enp0s8]: start running ordered scripts...
Today 09:24:40	DAEMON	INFO	localhost	nm-dispatcher[3900]:		Syslog	req:1 'dhcp4-change' [enp0s8]: new request (2 scripts)
Today 09:24:40	DAEMON	INFO	localhost	systemd[1]:		Syslog	Started Network Manager Script Dispatcher Service.
Today 09:24:40	DAEMON	INFO	localhost	dbus-daemon[745]:		Syslog	[system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Today 09:24:40	DAEMON	INFO	localhost	systemd[1]:		Syslog	Starting Network Manager Script Dispatcher Service...
Today 09:24:40	DAEMON	INFO	localhost	dbus-daemon[745]:		Syslog	[system] Activating via systemd: service name='org.freedesktop.nm_dispatcher' un...
Today 09:24:40	USER	INFO	localhost	NetworkManager[780]:		Syslog	<info> [1634027080.6841] dhcp4 (enp0s8): state changed bound -> bound
Today 09:24:40	USER	INFO	localhost	NetworkManager[780]:		Syslog	<info> [1634027080.6930] dhcp4 (enp0s8): expires in 600 seconds
Today 09:24:40	USER	INFO	localhost	NetworkManager[780]:		Syslog	<info> [1634027080.6926] dhcp4 (enp0s8): plen 24
Today 09:24:40	USER	INFO	localhost	NetworkManager[780]:		Syslog	<info> [1634027080.6925] dhcp4 (enp0s8): address 192.168.56.108 [localhost.localdomain]
Today 09:19:40	DAEMON	INFO	localhost	nm-dispatcher[3882]:		Syslog	req:1 'dhcp4-change' [enp0s8]: start running ordered scripts...
Today 09:19:40	DAEMON	INFO	localhost	nm-dispatcher[3882]:		Syslog	req:1 'dhcp4-change' [enp0s8]: new request (2 scripts)
Today 09:19:40	DAEMON	INFO	localhost	systemd[1]:		Syslog	Started Network Manager Script Dispatcher Service.
Today 09:19:40	DAEMON	INFO	localhost	dbus-daemon[745]:		Syslog	[system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Today 09:19:40	DAEMON	INFO	localhost	systemd[1]:		Syslog	Starting Network Manager Script Dispatcher Service...
Today 09:19:40	DAEMON	INFO	localhost	dbus-daemon[745]:		Syslog	[system] Activating via systemd: service name='org.freedesktop.nm_dispatcher' un...
Today 09:19:40	USER	INFO	localhost	NetworkManager[780]:		Syslog	<info> [1634026780.2472] dhcp4 (enp0s8): state changed bound -> bound
Today 09:19:40	USER	INFO	localhost	NetworkManager[780]:		Syslog	<info> [1634026780.2488] dhcp4 (enp0s8): expires in 600 seconds
Today 09:19:40	USER	INFO	localhost	NetworkManager[780]:		Syslog	<info> [1634026780.2485] dhcp4 (enp0s8): plen 24
Today 09:19:40	USER	INFO	localhost	NetworkManager[780]:		Syslog	<info> [1634026780.2484] dhcp4 (enp0s8): address 192.168.56.108 [localhost.localdomain]
Today 09:14:40	DAEMON	INFO	localhost	nm-dispatcher[3882]:		Syslog	req:1 'dhcp4-change' [enp0s8]: start running ordered scripts...
Today 09:14:40	DAEMON	INFO	localhost	nm-dispatcher[3882]:		Syslog	req:1 'dhcp4-change' [enp0s8]: new request (2 scripts)
Today 09:14:40	DAEMON	INFO	localhost	systemd[1]:		Syslog	Started Network Manager Script Dispatcher Service.
Today 09:14:40	DAEMON	INFO	localhost	dbus-daemon[745]:		Syslog	[system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Today 09:14:40	DAEMON	INFO	localhost	systemd[1]:		Syslog	Starting Network Manager Script Dispatcher Service...

To enable apache log:

```
# vim /etc/rsyslog.conf
```

```
local3.*                                                /var/log/httpd/error_log
local4.*                                               /var/log/httpd/access_log
```

```
# vi /etc/rsyslog.d/apache.conf
```

```
$ModLoad imfile

# Default Apache Error Log
$InputFileName /var/log/httpd/error_log
$InputFileTag httpd-error-default:
$InputFileStateFile stat-httpd-error
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor

# Default Apache Access Log
$InputFileName /var/log/httpd/access_log
$InputFileTag httpd-access-default:
$InputFileStateFile stat-httpd-access
$InputFileSeverity info
$InputFileFacility local4
$InputRunFileMonitor

$InputFilePollInterval 10
```

```
# systemctl restart rsyslog
```

Configuring the client system

Like the Rsyslog server, log in and check if the rsyslog daemon is running by issuing the command:

# systemctl status rsyslog

Next, proceed to open the rsyslog configuration file

```
# vi /etc/rsyslog.conf
```

At the end of the file, append the following line

```
*.* @192.168.20.120:514           # Use @ for UDP protocol
*.* @@192.168.20.120:514          # Use @@ for TCP protocol
```

Save and exit the configuration file. Just like the Rsyslog Server, open port 514 which is the default Rsyslog port on the firewall

```
# firewall-cmd  --add-port=514/tcp  --zone=public  --permanent
```

Next, reload the firewall to save the changes

```
# firewall-cmd --reload
```

Next, restart the rsyslog service

```
# systemctl restart rsyslog
```

To enable Rsyslog on boot, run following command

```
# sudo systemctl enable rsyslog
```

Enable Log in Cisco Router:

```
Router #
Router #config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#logging 192.168.20.120
Router(config)# service timestamps log datetime localtime show-timezone
msec
Router(config)# logging facility local3
Router(config)# logging trap warning
Router(config)# end
Router#show logging
```

Ref: https://www.ciscopress.com/articles/article.asp?p=426638&seqNum=3

Configure Syslog in Juniper:

```
cli
configure
set system syslog host 192.168.20.100 user info
set system syslog host 192.168.20.100 any info
set system syslog host 192.168.20.100 change-log notice
set system syslog host 192.168.20.100 interactive-commands notice
set system syslog host 192.168.20.100 match
"(UI_COMMIT:)|(UI_COMMIT_AT_COMPLETED)|(FLOW_SESSION_CREATE)|(FLOW_SESSION_DENY)|(FLOW_SESSION_CLOSE)"
set system syslog host 192.168.20.100 log-prefix <ID>
commit
```